5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/986,319	11/08/2001	Timothy J. Simms	16222.004	5579

28381 7590 03/07/2005

ARNOLD & PORTER LLP
ATTN: IP DOCKETING DEPT.
555 TWELFTH STREET, N.W.
WASHINGTON, DC 20004-1206

EXAMINER	
ANANTHANARAYANAN, RAMYA	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/986,319	**Applicant(s)** SIMMS, TIMOTHY J.
	Examiner Ramya Ananthanarayanan	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-152* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-152* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☒ Other: *Copy of Renumbered Claims*.

1. Claims 1-152 have been examined.

2. The preliminary amendment submitted by applicant was not entered. The Patent and Trademark Office renumbered the claims submitted by the applicant in order to repair issues of claims with duplicate claim numbers. A set of renumbered claims is attached for applicant to view. Applicant must amend the claims in order to repair any issues with dependencies in the claims. For example, in the renumbered claims, claim 15 depends upon claim 13, but should depend upon claim 14. The examiner treated the claims with respect to this office actions as per the intentions of applicant as interpreted through the preliminary amendment. Applicant should amend the claims appropriately.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 23 recites the limitation "the method of claim 22" in line 1. There is insufficient antecedent basis for this limitation in the claim because claim 22 refers to a signal. The examiner will treat the claim as referring to "the signal of claim 22".

5. Claim 89 recites the limitation "said first key" in line 2. There is insufficient antecedent basis for this limitation in the claim because claim 85 refers to a second key. The examiner will treat the claim as referring to 'said second key'.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 13-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed towards a digital signal, which is not considered statutory subject matter.

8. To expedite a complete examination of the application, the claims rejected under 35 U.S.C. 101 (non-statutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 1, 4-11, 13-16, 18, 20, 21, 24-36, 39, 40, 43-45, 47-51, 57-89, 112-121, 124-131, 133-137, and 144-147 are rejected under 35 U.S.C. 102(b) as being anticipated by Bellovin et al. (U.S. Patent 5,421,599).

11. With respect to claim 1, Bellovin et al. disclose a method for obtaining a shared secret key, comprising the steps of:

Identifying a first shared random number (column 6, lines 52-54, lines 62-67);

Identifying a second shared random number (column 6, lines 57-59; column 7, lines 2-10); and

Obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

12. With respect to claim 4, Bellovin et al. disclose a method for obtaining a shared secret key utilized in a network having at least a first computer and a second computer, said method comprising the steps of:

Transmitting a first message from said first computer to said second computer, said first message including a first shared random number (column 6, lines 52-54, lines 62-67);

Generating a second shared random number in said second computer (column 6, lines 57-59; column 7, lines 2-10); and

Generating a shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

13. With respect to claim 24, Bellovin et al. disclose a method for obtaining a shared secret key, comprising the steps of:

Receiving a first message including a first shared random number (column 6, lines 52-54, lines 62-67);

Identifying a second shared random number (column 6, lines 57-59; column 7, lines 2-10); and

Obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

14. With respect to claims 57, 71, 72, and 81, Bellovin et al. disclose a device including at least one processor (column 14, line 26: It is inherent in a computer to have a processor that executes the instructions in the memory of the computer.), said at least one processor executing software instructions for obtaining a shared secret key, said software instructions comprising a software module parsing a first message including a first shared random number to identify said first shared random number (column 6, lines 52-54, lines 62-67), identifying a second shared random number (column 6, lines 57-59; column 7, lines 2-10), and obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26), wherein the device is capable of transforming messages using the shared secret key (column 7, lines 22-26).

15. With respect to claim 112, Bellovin et al. disclose a method for obtaining a shared secret key, comprising the steps of:

Identifying a first shared random number (column 6, lines 52-54, lines 62-67);

Receiving a second message including a second shared random number (column 6, lines 57-59; column 7, lines 2-10); and

Obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

16. With respect to claim 13, Bellovin et al. disclose an electronic data signal (column 5, lines 10-11: The communication is conducted over telephone lines, meaning that data must be transmitted through a continuous transmission signal.) including information encoded using a shared secret key, wherein said shared secret key is obtained from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

17. With respect to claim 14, Bellovin et al. disclose an electronic data signal, wherein said data signal is propagated through a network (column 5, lines 10-11: The communication is conducted over telephone links, meaning that data must be transmitted through the telephony network.)).

18. With respect to claim 15, Bellovin et al. disclose an electronic data signal, wherein said information is encoded using said shared secret key (column 7, lines 23-26).

19. With respect to claim 16, Bellovin et al. disclose an electronic data signal, wherein said information is encrypted using said shared secret key (column 7, lines 23-26).

20. With respect to claim 18, Bellovin et al. disclose an electronic data signal, wherein said signal is a wireless signal (column 15, lines 39-40: The cellular telephone industry uses wireless, digital signals.).

21. With respect to claim 20, Bellovin et al. disclose an electronic data signal, wherein said signal is propagated as an analog signal (column 5, lines 10-11: The communication is conducted over telephone lines, meaning that data must be transmitted through a continuous transmission signal. That type of signal is an analog signal.).

22. With respect to claim 21, Bellovin et al. disclose an electronic data signal, wherein said signal is propagated as a digital signal (column 15, lines 39-40: The cellular telephone industry uses wireless, digital signals.).

23. With respect to claims 5 and 25, Bellovin et al. disclose a method, further comprising the step of transmitting a second message from said second computer to said first computer, said second message including said second shared random number (column 6, lines 52-54, lines 62-67).

24. With respect to claim 26, Bellovin et al. disclose a method, wherein said step of identifying a second shared random number comprises generating said second shared random number (column 6, lines 57-59; column 7, lines 2-10).

25. With respect to claim 75, Bellovin et al. disclose a device, wherein said device transmits a second message including the second shared random number (column 7, lines 2-10).

26. With respect to claim 84, Bellovin et al. disclose a method, wherein said software module generates a first message including said first shared random number (column 6, lines 62-67).

27. With respect to claim 85, Bellovin et al. disclose a method, wherein said first message also includes a second key (column 6, lines 52-54).

28. With respect to claim 113, Bellovin et al. disclose a method, further comprising the step of transmitting a first message including said first shared random number (column 6, lines 52-54, lines 62-67).

29. With respect to claim 133, Bellovin et al. disclose a method, further comprising receiving information identifying a user (column 5, lines 29-30).

30. With respect to claim 134, Bellovin et al. disclose a method, wherein said first key is associated with said user (column 5, lines 18-27).

31. With respect to claim 135, Bellovin et al. disclose a method, wherein said first key corresponds to a password known by said user (column 5, lines 18-27).

32. With respect to claims 6, 27, 28, 30, 39, 76, 89, 115, 118, 119, and 136, Bellovin et al. disclose a method, wherein said first message is encoded using a first key obtained using information obtained from a password. (column 5, lines 18-29; column 13, lines 18-20).

33. With respect to claims 7, 8, 29, 31, 40, 77, 116, 120, and 137, Bellovin et al. disclose a method, wherein said step of encoding said first message comprises encrypting said first message using said encoded password (column 5, lines 18-29; column 13, lines 18-20).

34. With respect to claims 9 and 78, Bellovin et al. disclose a method, wherein said first message also includes an asymmetric key (column 5, lines 18-29).

35. With respect to claims 32, 49, 117, and 144, Bellovin et al. disclose a method, wherein said first message also includes a second key (column 6, lines 52-54).

36. With respect to claims 33, 50, 86, 124, and 145, Bellovin et al. disclose a method, wherein said second key is an asymmetric key (column 5, lines 18-29).

37. With respect to claims 10, 34, 51, 79, 87, 125, and 146, Bellovin et al. disclose a method, wherein said second message is encoded using said asymmetric key (column 5, lines 33-41).

38. With respect to claims 11, 35, 80, 88, 126, and 147, Bellovin et al. disclose a method, wherein said second message is encrypted using said asymmetric key (column 5, lines 33-41).

39. With respect to claims 36 and 43, Bellovin et al. disclose a method, further comprising receiving said password from a user (column 1, line 49).

40. With respect to claims 44 and 48, Bellovin et al. disclose a method, further comprising transmitting information identifying said user (column 1, line 46).

41. With respect to claim 45, Bellovin et al. disclose a method, wherein said user is a human user (column 3, lines 13).

42. With respect to claim 47, Bellovin et al. disclose a method, further comprising decrypting said first message using information obtained from said password (column 5, lines 33-35).

43. With respect to claim 58, Bellovin et al. disclose a device, wherein the first shared random number is communicated to a user (column 6, lines 52-54, lines 62-67).

44. With respect to claim 59, Bellovin et al. disclose a device, wherein the shared secret key is obtained from said user (column 6, lines 57-59; column 7, lines 2-10).

45. With respect to claim 60, Bellovin et al. disclose a device, wherein the shared secret key is obtained from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

46. With respect to claim 61, Bellovin et al. disclose a device, wherein said step of identifying a first shared random number comprises generating said first shared random number (column 6, lines 52-54, lines 62-67).

47. With respect to claim 62, Bellovin et al. disclose a device, wherein said step of identifying a second shared random number comprises receiving a second message including said second shared random number (column 6, lines 57-59; column 7, lines 2-10).

48. With respect to claims 63 and 74, Bellovin et al. disclose a device, wherein said step of identifying a second shared random number comprises generating said second shared random number (column 6, lines 57-59; column 7, lines 2-10).

49. With respect to claim 64, Bellovin et al. disclose a device, wherein said step of identifying a first shared random number comprises receiving a first message including said first shared random number (column 6, lines 57-59; column 7, lines 2-10).

50. With respect to claim 65, Bellovin et al. disclose a device, wherein said device is capable of transforming messages by encoding messages using the shared secret key (column 7, lines 22-26).

51. With respect to claim 66, Bellovin et al. disclose a device, wherein said encoding messages using the shared secret key comprises encrypting messages using the shared secret key (column 7, lines 22-26).

52. With respect to claim 67, Bellovin et al. disclose a device, wherein said device is capable of transforming messages by decoding messages using the shared secret key (column 7, lines 22-26).

53. With respect to claim 68, Bellovin et al. disclose a device, wherein said decoding messages using the shared secret key comprises decrypting messages using the shared secret key (column 7, lines 22-26).

54. With respect to claim 69, Bellovin et al. disclose a device, wherein said device comprises a computer (column 14, line 26).

55. With respect to claim 70, Bellovin et al. disclose a device, wherein said device comprises a handheld device (column 15, lines 39-40).

56. With respect to claims 73 and 82, Bellovin et al. disclose a device, wherein said device decrypts said first message (column 7, line 2).

57. With respect to claim 83, Bellovin et al. disclose a method, wherein said step of identifying a first shared random number comprises generating said first shared random number (column 6, lines 62-67).

58. With respect to claim 114, Bellovin et al. disclose a method, wherein said step of identifying a first shared random number comprises generating said first shared random number (column 6, lines 52-54, lines 62-67).

59. With respect to claim 121, Bellovin et al. disclose a method, wherein said step of obtaining the shared secret key comprises obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

60. With respect to claim 127, Bellovin et al. disclose a method, further comprising decoding said second message (column 5, lines 42-45).

61. With respect to claim 128, Bellovin et al. disclose a method, wherein said decoding said second message comprises decoding said second message using a third key (column 5, lines 42-45).

62. With respect to claim 129, Bellovin et al. disclose a method, wherein said third key and said second key form an asymmetric key pair (column 5, lines 18-20).

63. With respect to claim 130, Bellovin et al. disclose a method, further comprising the step of generating said asymmetric key pair (column 5, lines 18-20).

64. With respect to claim 131, Bellovin et al. disclose a method, wherein said asymmetric key pair is generated dynamically (column 5, lines 18-20).

Claim Rejections - 35 USC § 103

65. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

66. Claims 2, 3, 12, 22, 23, 37, 38, 52, 90-111, 122, 123, 152 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (U.S. Patent 5,241,599) in view of Shona et al. (U.S. Patent 6,018,581).

67. Bellovin et al. and Shona et al. are analogous art because both are in the field of electronic communication.

68. With respect to claim 90, Bellovin et al. disclose the steps of:

Encoded computer means for identifying a first shared random number (column 6, lines 52-54, lines 62-67);

Encoded computer means for identifying a second shared random number (column 6, lines 57-59; column 7, lines 2-10); and

Encoded computer means for obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

69. Bellovin et al. does not disclose a machine-readable storage medium containing instructions for a processor, said instructions being the steps for the processor, comprising the aforementioned steps.

Shona et al. disclose a machine-readable storage medium containing instructions for a processor, said instructions being the steps for the processor, comprising the aforementioned steps (column 2, lines 56-59).

70. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Shona et al. with the teachings of Bellovin et al. in order to make a communication system which makes communication harder to alter or forge (column 2, lines 51-54).

71. With respect to claim 2, 12, 22, 37, 92, and 122, Bellovin et al. does not disclose a method, wherein said combining function includes a logical function.
Shona et al. disclose a method, wherein said combining function includes a logical function (column 6, lines 12-16, lines 22-25).

72. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Shona et al. with the teachings of Bellovin et al. in order to make the encryption key greatly varied (column 6, lines 25-29).

73. With respect to claim 3, 23, 38, 93, 123, and 152, Bellovin et al. does not disclose a method, wherein said logical function includes an exclusive or (XOR) function.
Shona et al. disclose a method, wherein said logical function includes an exclusive or (XOR) function (column 6, lines 12-16, lines 22-25).

74. The motivation for combining the teachings of Shona et al. with the teachings of Bellovin et al. is disclosed above.

75. With respect to claim 52, Bellovin et al. disclose a method of claim 37, wherein said second message is encrypted with said second key (column 5, lines 33-41).

76. With respect to claim 91, Bellovin et al. does not disclose a storage medium wherein said storage medium is at least one of a group including semiconductor memory device, magnetic device, optical device, magneto-optical device, floppy diskette, hard drive, CD-ROM, magnetic tape, computer memory, and memory card.
Shona et al. disclose a storage medium wherein the storage medium is a computer memory (column 2, lines 56-57).

77. The motivation for combining the teachings of Shona et al. with the teachings of Bellovin et al. is disclosed above.

78. With respect to claim 94, Bellovin et al. disclose the steps of:

Encoded computer means for parsing a first message including a first shared random number to obtain said first shared random number (column 6, lines 52-54, lines 62-67);

Encoded computer means for identifying a second shared random number (column 6, lines 57-59; column 7, lines 2-10); and

Encoded computer means for obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

79. Bellovin et al. does not disclose a machine-readable storage medium containing instructions for a processor, said instructions being the steps for the processor mentioned above.

Shona et al. disclose a machine-readable storage medium containing instructions for a processor, said instructions being the steps for the processor mentioned above (column 2, lines 56-59).

80. The motivation for combining the teachings of Shona et al. with the teachings of Bellovin et al. is disclosed above.

81. With respect to claim 95, Bellovin et al. disclose a storage medium, further comprising encoded computer means for decrypting said first message (column 7, line 2).

82. With respect to claim 96, Bellovin et al. disclose a storage medium, further comprising encoded computer means for generating a second message including said second shared random number (column 6, lines 57-59; column 7, lines 2-10).

83. With respect to claim 97, Bellovin et al. disclose a storage medium, wherein said first message is encoded using a first key obtained using information obtained from a password (column 5, lines 18-29; column 13, lines 18-20).

84. With respect to claim 98, Bellovin et al. disclose a storage medium, wherein said first message is encrypted using a first key obtained using information obtained from a password (column 5, lines 18-29; column 13, lines 18-20).

85. With respect to claim 99, Bellovin et al. disclose a storage medium, wherein said first message also includes an asymmetric key (column 5, lines 18-29).

86. With respect to claim 100, Bellovin et al. disclose a storage medium, wherein said second message is encoded with said asymmetric key (column 5, lines 33-41).

87. With respect to claim 101, Bellovin et al. disclose a storage medium, wherein said second message is encrypted with said asymmetric key (column 5, lines 33-41).

88. With respect to claim 102, Bellovin et al. disclose the steps of:

Encoded computer means for identifying a first shared random number (column 6, lines 52-54, lines 62-67);

Encoded computer means for parsing a second message including a second shared random number to obtain said second shared random number (column 6, lines 57-59; column 7, lines 2-10); and

Encoded computer means for obtaining the shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 7, lines 22-26).

89. Bellovin et al. does not disclose a machine-readable storage medium containing instructions for a processor, said instructions being the steps for the processor mentioned above.

Shona et al. disclose a machine-readable storage medium containing instructions for a processor, said instructions being the steps for the processor mentioned above (column 2, lines 56-59).

90. The motivation for combining the teachings of Shona et al. with the teachings of Bellovin et al. is disclosed above.

91. With respect to claim 103, Bellovin et al. disclose a storage medium, further comprising encoded computer means for decrypting said second message (column 5, lines 42-43).

92. With respect to claim 104, Bellovin et al. disclose a storage medium, further comprising encoded computer means for transmitting a first message including said first shared random number (column 6, lines 52-54, lines 62-67).

93. With respect to claim 105, Bellovin et al. disclose a storage medium, wherein said first message also includes a second key (column 6, lines 52-54).

94. With respect to claim 106, Bellovin et al. disclose a storage medium, wherein said second key is an asymmetric key (column 5, lines 18-29).

95. With respect to claim 107, Bellovin et al. disclose a storage medium, wherein said second message is encoded with said asymmetric key (column 5, lines 33-41).

96. With respect to claim 108, Bellovin et al. disclose a storage medium, wherein said second message is encrypted with said asymmetric key (column 5, lines 33-41).

97. With respect to claim 109, Bellovin et al. disclose a storage medium, wherein said first message is encoded using a first key (column 5, lines 18-29; column 13, lines 18-20).

98. With respect to claim 110, Bellovin et al. disclose a storage medium, wherein said first message is encrypted using a first key (column 5, lines 18-29; column 13, lines 18-20).

99. With respect to claim 111, Bellovin et al. disclose a storage medium, wherein said first key corresponds to a password known by a user (column 5, lines 18-29; column 13, lines 18-20).

100. Claims 17, 41, 42, 46, 138-141 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (U.S. Patent 5,241,599) in view of Wu (U.S. Patent 6,539,749).

101. Bellovin et al. and Wu are analogous art because both are in the field of electronic communication.

102. With respect to claim 17, Bellovin et al. disclose a signal (column 5, lines 10-11: The communication is conducted over telephone lines, meaning that data must be transmitted through a continuous transmission signal.).

103. Bellovin et al. do not disclose a signal wherein said signal comprises a packet of data representing a portion of said information.

Wu discloses a signal, wherein said signal comprises a packet of data representing a portion of said information (column 3, lines 62-63: If one has the ability to intercept packets that make up messages transmitted from one person to another on the network, that necessarily means packets of information are used to represent a portion of information.).

104. It would have been obvious to one of ordinary skill to combine the teachings of Wu with the teachings of Bellovin et al. because it is well known in the art to send information over a data network through packets.

105. With respect to claim 41, Bellovin et al. do not disclose a method, wherein said encrypted password is obtained from an output of a one-way function having an input including said password.

Wu discloses a method, wherein said encrypted password is obtained from an output of a one-way function having an input including said password (column 5, lines 48-52).

106. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Wu with the teachings of Bellovin et al. in order to enable the server which the user is trying to access to determine if the user knows the password for the account specified during login (column 5, lines 42-45).

107. With respect to claim 42, Bellovin et al. do not disclose a method, wherein said one-way function is a hash function.

Wu discloses a method, wherein said one-way function is a hash function (column 5, lines 48-52).

108. The motivational benefits of combining the teachings of Wu with the teachings of Bellovin et al. are disclosed above.

109. With respect to claims 46 and 138, Bellovin et al. do not disclose a method, further comprising the step of obtaining said first key from an output of a one-way function having an input including said password.

Wu discloses a method, further comprising the step of obtaining said first key from an output of a one-way function having an input including said password (column 5, lines 42-45).

110. The motivational benefits of combining the teachings of Wu with the teachings of Bellovin et al. are disclosed above.

111. With respect to claim 139, Bellovin et al. do not disclose a method, further comprising the step of obtaining said first key by looking up said user in a password file. Wu discloses a method, further comprising the step of obtaining said first key by looking up said user in a password file (column 3, lines 33-37).

112. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Wu with the teachings of Bellovin et al. in order to verify that the user asking to log onto a server is who the person claims to be (column 3, lines 23-25).

113. With respect to claim 140, Bellovin et al. do not disclose a method, wherein said password file contains an encoded password.

Wu discloses a method, wherein said password file contains an encoded password (column 3, lines 33-37).

114. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Wu with the teachings of Bellovin et al. in order to verify a user's asserted password without having to reveal the user's password (column 3, lines 35-37).

115. With respect to claim 141, Bellovin et al. do not disclose a method, wherein said encoded password is an encrypted password.
Wu discloses a method, wherein said encoded password is an encrypted password (column 3, lines 33-37).

116. The motivational benefits of combining the teachings of Wu with the teachings of Bellovin et al. are disclosed above.

117. Claims 142 and 143 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (U.S. Patent 5,241,599) and Wu (U.S. Patent 6,539,479) in view of Kung et al. (U.S. Patent 5,434,918).

118. Bellovin et al., Wu, and Kung et al. are all analogous art because all are in the field of electronic communications.

119. With respect to claim 142, Bellovin et al. and Wu do not disclose a method, wherein said password file is encoded.

Kung et al. disclose a method, wherein said password file is encoded (column 3, lines 26-29).

120. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Kung et al. with the combined teachings of Bellovin et al. and Wu in order to protect the password file (column 3, line 24).

121. With respect to claim 143, Bellovin et al. and Wu do not disclose a method, wherein said encoded password file is an encrypted password file.
Kung et al. disclose a method, wherein said encoded password file is an encrypted password file (column 3, lines 26-29).

122. The motivational benefits of combining the teachings of Kung et al. with the combined teachings of Bellovin et al. and Wu are disclosed above.

123. Claims 54-56, 132, 148-151, and 153 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (U.S. Patent 5,241,599) in view of Gutowitz (U.S. Patent 5,365,589).

124. Bellovin et al. and Gutowitz are analogous art because both are in the field of electronic communication.

125. With respect to claims 54 and 149, Bellovin et al. do not disclose a method, wherein said first message also includes a timestamp.

Gutowitz discloses a method, wherein said first message also includes a timestamp (column 32, lines 31-34).

126. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Gutowitz with the teachings of Bellovin et al. in order to provide application-specific parameters so as not to redundantly send information (column 32, lines 18-37).

127. With respect to claims 55 and 150, Bellovin et al. disclose a method, wherein said first message also includes a second key (column 6, lines 52-54).

128. Bellovin et al. do not disclose a method, wherein said first message also includes a timestamp.

Gutowitz discloses a method, wherein said first message also includes a timestamp (column 32, lines 31-34).

129. The motivational benefits of combining the teachings of Gutowitz with the teachings of Bellovin et al. are disclosed above.

130. With respect to claims 56 and 151, Bellovin et al. disclose a method, wherein said second key is an asymmetric key (column 5, lines 18-29).

131. With respect to claim 132, Bellovin et al. do not disclose a method, wherein said asymmetric key pair is selected from a set of pre-generated asymmetric key pairs.
Gutowitz discloses a method, wherein said asymmetric key pair is selected from a set of pre-generated asymmetric key pairs (Abstract, lines 10-12; column 3, lines 59-60).

132. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Gutowitz with the teachings of Bellovin et al. in order to make code breaking and tampering with the encryption more difficult (column 3, lines 54-60).

133. With respect to claims 148 and 153, Bellovin et al. do not disclose a method, wherein said second message also includes a timestamp.
Gutowitz discloses a method, wherein said second message also includes a timestamp (column 32, lines 31-34).

134. The motivational benefits of combining the teachings of Gutowitz with the teachings of Bellovin et al. are disclosed above.

135. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (U.S. Patent 5,241,599) in view of Whitmire (6,115,817).

136. Bellovin et al. and Whitmire are analogous art because both are in the field of electronic communications.

137. With respect to claim 19, Bellovin et al. do not disclose a signal, wherein the signal is embedded in a carrier wave.

Whitmire disclose a signal, wherein the signal is embedded in a carrier wave (column 4, lines 45-65).

138. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Whitmire with the teachings of Bellovin et al. in order to not limit the forms in which the invention could be implemented (column 4, lines 45-65).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ramya Ananthanarayanan whose telephone number is (571) 272-5860. The examiner can normally be reached on Monday through Friday, 8:30 -5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RA

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER